# MARKETING & IMPLEMENTING COMPUTER SECURITY

Mark Wilson
National Institute of Standards & Technology
Building 820, Room 426
Gaithersburg, MD  20899

I had spent several years in a previous job trying to convince computer system users and managers that they should practice good computer security.  Finally, shortly before leaving that job, I saw signs that people were listening and responding.  I overheard executive-level and senior managers discussing the importance of installing anti-virus software, ensuring software copyright compliance, and accrediting systems.  They were speaking in a manner which indicated they thought it to be their responsibility to ensure these tasks were accomplished.

Initially, I thought these events to be strange; these people were talking about my responsibilities as if they were their responsibilities.  It finally struck me that I was seeing some positive results of my four-year-long attempt to get people to integrate some of the computer security tasks which I had been preaching and writing about into their regular day's work.

## A Commonly-Held View of Computer Security

For years my job was thought of by others to be an unwelcome and possibly not even a necessary evil.  It was easy to see how people perceived computer security in such a negative manner.  Many computer security programs are born soon after an inspector general's (IG's) visit during which an agency is cited for not having a required program.  Some agencies begin a computer security program following a major security incident, or just prior to an IG visit, hoping to avoid yet another adverse finding.  In many cases, the embryonic computer security program is placed under an established program (e.g., IRM or physical security) for protection and nurturing while the program matures.  Other times, the new program is "thrown to the wolves" - placed in the agency where it must fight for credibility and survival from the very beginning. Regardless of where the new security program is placed, the general perception throughout the agency is that this new program:

* is the result of a kneejerk management reaction;

* is just another overhead function (e.g., costs too much and takes away valuable resources that could be better used to do the real job of an agency);

* does not help other traditional agency functions do their job; and, therefore

* is not necessary and should not be taken seriously.

This is what I faced when I began my computer security career.

These perceptions were reinforced on a regular basis by data processing managers, computer specialists in the data center, systems planning specialists, functional managers (data owners), and end users. On one occasion I was in a system implementation planning meeting with managers and analysts from data processing, systems planning, contracting, training, and the end user's shop. The local project manager was on the speaker phone with the function manager at our main office, when the function manager mentioned there was a "computer security troublemaker down there" who had raised a stink over what we in the computer security office had seen as a potentially troublesome aspect of connectivity within the proposed new system. I was that troublemaker.

## Do Not Allow Others to Shape Your View of Computer Security

For some time, partly because of the initial responses to the new computer security program, I allowed myself to believe that the job of "doing" computer security was somehow outside the mainstream of "doing" agency business. It was only through hard-headed determination that I was able to get invited (or invite myself) to senior management meetings, to meet with project managers, and convince some managers and users, though certainly not all, that they needed to "do" computer security.

## An Approach That Works

I began to change the tack I took when "selling" computer security. I realized there are some parts of the job that only the computer security program officer/ manager can do, for example, developing the section of the annual report which shows the status of the security program, maintaining the system accreditation and certification program, providing a head count of personnel with collateral-duty assignments in helping to accomplish computer security tasks, and providing advice and knowledge of available controls and security tools. However, the real work in the computer security program were the day-to-day details, and that was really someone else's job. It was the functional managers', supervisors', system and data owners', and users' job to do computer security. All I had to do was show them the following:

* what has to be done;

* why it is their job to do it;

* why it is in their best interest to do it; and finally,

* how to do it.

In addition to serving as the agency's Computer Security Officer, I managed a small data processing/information technology (IT) shop. We supported users of microcomputers, LANs, and minicomputers. I managed computer security and the computer support functions, including life cycle management (LCM) and the computer-related portions of the agency's annual business plan and IT budget.  With a relatively small staff, including some people physically located in and working for other departments, the challenge quickly became finding a way to get all of the important work completed.  Microcomputer and LAN support (customer support) was a top priority.  But so was LCM, since without prior documentation and LCM approval for a new system or systems, funding would not be provided by the ADP/IT budget shop at our headquarters office.  Getting some very visible and required computer security tasks completed (e.g., password and access control hardware and software installed on systems, installing anti-virus and access warning message software) was also necessary.  It is always useful to have concrete accomplishments early in a program.

When I arrived at that job in 1988, computer specialists and assistants were providing customer support.  No one was managing or doing computer security, LCM, or IT-related budgeting.  I had heard horror stories in the past about computer security officers spending all of their time "doing" computer security - changing cypher locks, mailing out passwords in envelopes every quarter, and installing password/access control and anti-virus software.  These tasks should have been accomplished by computer support staff and/or people who had collateral-duty computer security responsibilities.  In my first meetings with executive level and senior managers, I explained that my plan for computer security included those tasks I would do and those tasks staff and computer security collateral-duty personnel would do.

## You Must First Get Executive-Level Buy-In

The first "sell" was that I could not do it all, that I had been hired to manage the program, and that there was a long list of requirements - too long a list for one person to accomplish.  It was probably to my benefit that I was hired four months before a visit by the inspector general (IG).  My audience knew there was a lot of work to do; they had hired me at the last minute to bail them out.  Virtually no work had been done in the three years since the last inspection.  Selling senior management on the concept of how I would get the work done was not as difficult in this case.  In this instance, the agency - specifically, the Commanding Officer and Executive Officer - had hired me as the expert.  They expected and trusted me to know how to get the work done.  Conversely, if my position had been filled from within the agency, that person would have to gain experience and knowledge before they would have gained credibility.  Until then, every recommendation and action may have had to be justified many times over.

Executives and senior managers are more likely to be responsive to the need for computer security since they can see the harm a breach of security can do to an organization.  Functional managers are more focused on resource issues, and will usually need to be sold on the idea of improving their program and not putting their resources at risk.  However, after senior management buy-in, functional managers' requests for computer security-related resources may be better received and funded.

Selling what had to be done also went well. I did not glaze their eyes over by rattling off all the well known computer security terms and tasks - security plans, accreditation / certification, identification and authentication, auditability, risk analysis, contingency planning, etc. - the all-too-often poorly explained concepts, requirements, and related paperwork that give many managers the perception that we may, indeed, be un-necessary evils. I donned the "plaid used car salesperson's jacket" and told them what they wanted to hear, and then what they needed to hear. What they wanted to hear was that I had a plan for starting the computer security program, and that the plan could be put in place before the IG visit.

What they needed to hear took a little longer. I began by defining a very important phrase - "computer security". I told them the program should be called "data integrity" or "system integrity," leaving out the word "security." I mentioned that I did not approach the job from a "locks, bars, and guard dogs" perspective, that is, from a traditional physical security program perspective. I did not say this to discount the importance of the physical security aspects of the computer security program, but rather to break down the often pre-conceived negative notion of any program that contains the word "security."

Shortly after I arrived we began to purchase a significant number of microcomputers for the office. The agency's Commanding Officer was already concerned with the increasing value of the hardware and software for which he was responsible. Physical security of these resources was an easy sell. He asked me about a PC-based access control system to control physical access to the offices. He had identified and accepted his responsibility for this aspect of security. Naturally, I agreed with his solution. It was well thought out and appeared to mitigate the threat posed by a less-than-adequate door lock. As valuable as a risk analysis can be to identify the proper control for a particular threat, in some cases (e.g., when the agency director buys-in to your computer security program, has a viable solution to a problem, has the funding, and is volunteering to fund the project) it is prudent to implement it.

## Building Credibility Builds a Credible Security Program

A key task and perhaps the most important part of managing a computer security program is building your own credibility. You must make sense to executives and senior management in order for middle management and supervisors to take you and your program seriously. You have to make sense to all these managers before users and operators will integrate security into how they accomplish their jobs. As in the example I have used throughout this paper, the first meetings with executives and senior management are the most important. These first impressions will probably last as long as you are in your position, or as long as these managers are with your agency. A good start can pave the long road you face and make the struggle easier. Conversely, a bad beginning can almost guarantee a difficult, if not impossible, future for you and your security program.

### Make Computer Security the Managers' & Users' Job

Some of our systems processed and stored information subject to the Privacy Act of 1974, as well as sensitive management, financial/budget, proprietary, and privileged information. I explained that management had a legal responsibility to adequately protect sensitive information, and then mentioned the Privacy Act and Computer Security Act requirements and penalties. In addition to the data sensitivity issues, I mentioned that the information in the systems was their information in their systems. I mentioned that if their information was important enough or voluminous enough to justify the purchase of a microcomputer to store, process and manage the data, and that if the information were not available to them when they needed it, or the printed output was not what they had expected, that the accomplishment of their mission or the agency's mission might be adversely affected.

I planted ideas about knowing and controlling who was using their systems, whether their data was being backed up, and how their important work would be accomplished if the systems could not be used. I followed up with conversations about protecting their systems with password and access control hardware and software, backups, and contingency planning, and tied those requirements to the previous conversation. Following on the heels of why it made sense (or should make sense) to managers to protect systems, introducing these concepts was reasonably well received. I wanted to get them thinking about their data as being very closely related to their job. I wanted to persuade them to begin taking their data and its security seriously, and that computer security is not something new to them, it is just another aspect of responsible management. In time, I was able to convince most managers.

### Select Your Battles - Pick the Fights You Can Win

I mentioned the software copyright license issue. This was another real-world issue management could understand. They had a legal responsibility to ensure that people in their charge understood and complied with software copyright licenses for the software they used. I explained it, not as something new to worry about, but as something we should have managed all along. I drove the point home by giving examples of cases in which vendors' lawyers sat across the table from government lawyers discussing violations of copyright licenses and the penalties that could be levied. During the first discussion on this subject, senior management dictated on-the-spot that we would make sure we were legal and stayed legal. This up-front understanding and support by senior management paid off later. During follow-up meetings with functional managers I explained the need to upgrade off-the-shelf software, or buy additional copies for new users. I went into such meetings "dual-hatted" - computer security officer and data processing director. Rarely did I have to re-visit my "sales pitch" on the need to comply with copyright licenses. The biggest battle was whether the functional manager would use his or her funds, or whether I would purchase the software from the computer operations and security budget. In cases where the funds were not available we would approach senior management. The discussion and decision never included circumventing the terms of the copyright license. Granted, it was easier in this case being dual-hatted, but when presented with a clear picture of what must be done, and with senior management's support, most managers, even data processing directors, can make the computer security job easier.

We discussed acquiring battery backup devices for minicomputers, LAN servers, and critical microcomputers in the office. We also determined that purchasing a surge suppressor with each new system or purchasing one for each existing system was such an easy way to protect systems and data. The Commanding Officer and Executive Officer mandated that each system would have a surge suppressor. Requests for the necessary funding for battery backup systems and surge suppressors, as well as other computer security resources (e.g., anti-virus software, PC-based access control software and hardware, and LAN-based software monitoring and audit trail software), became part of the activity's business plan and became items that the Executive-level managers fought for during annual budget negotiations.

Later, as computer viruses became more prevalent, and television and newspapers covered this new threat, I began briefing top management and functional managers, as well as users, about viruses and about how <u>they</u> could prevent virus attacks. With all the media coverage and some successful attacks on some of our systems, the job of convincing top management of the need for local policy and procedures, training, and disciplinary action (when deserved) was an easy task. Management clearly understood the impact on their job or mission which had resulted or could result from the loss of data, processing time and labor. Often my pitch during the Commanding Officer's morning meeting was preempted by my boss advising his department directors and other managers of the latest virus attack or the latest discovery of an infected diskette, before it became an attack. He presented the same news I had passed to him that day or the previous day. He took the matter quite seriously; he viewed computer security vulnerabilities as another threat to doing business. He took it as his job.

Managers clearly understood that when their boss declared a new security policy or verbally reinforced his existing policy and procedures, it was in their best interest to follow his example. Hearing a warning from the Commanding Officer carried that extra amount of clout, beyond hearing it from the computer security officer. This worked especially well in those few cases in which I could not convince the functional manager of the importance of following agency policy. During five quarterly "Captain's Calls" (agency-wide, "all hands" meetings) in the last two years of my tour at that agency, Commanding Officers presented awards and certificates to computer specialists and users who prevented virus attacks by scanning diskettes, promptly reporting the discovery of viruses, and performed other noteworthy security and computer operations tasks. One award was monetary; the others were individualized and highly-coveted coffee mugs. During those years, my staff and collateral-duty security appointees vied for this form of recognition. Their supervisors and managers shared the spotlight when an employee was selected by senior management for an award. By successfully selling the need for vigilance, along with developing reasonable policy and procedures, and training managers and users, the anti-virus portion of the computer security program, for example, took on a life of its own. It literally ran - or could have run - without me.

It is important that users believe they will be rewarded, not punished, for bringing attention to computer security problems. A reward system makes people want to report incidents or unusual events, instead of trying to hide problems or ignore potential problems. Rewarding people for computer security awareness has the added benefit of making management aware that threats do not disappear even if you have a computer security program in place.

Citing aspects of the computer security program that managers could understand got their attention and their acceptance, for the most part. I had used the "appeal to reason" approach - how their jobs and blood pressure could be affected by a preventable system failure, data integrity problems, or the inappropriate disclosure of certain information. I then mentioned in an "oh, by the way" manner, references to federal law. Just telling managers they had to do something because of an instruction from higher authority had never "sold the car" in the past. Adding the eye-glazing computer security buzzwords and phrases never held their attention, either. As I entered a discussion with managers and users whose expertise was in subjects other than computer operations or security, I reminded myself that I had to translate our profession's jargon into terms that the listener could grasp. Although this is generally thought to be nothing more than a good communication skill, it can make the difference between being understood, accepted, and successful, or being misunderstood, ignored, and perceived to be a failure. The direction of an agency's computer security program is often directly related to the agency's perception and treatment of the security program manager.

## Get the Right People to do Computer Security

In order that I could concentrate on "managing" computer security and other functions, I added microcomputer, LAN, and minicomputer security tasks to my computer support staff's daily and weekly list of projects. By making computer security tasks just another part of the job, the following three audiences saw the integration of security disciplines which many people had perceived to be separate functions:

* The computer specialists and assistants began to view the security work as just another item on the continuous list of things to do;

* System users saw the computer support people dealing with security issues; and

* Managers and supervisors saw more people than I doing computer security.

This reinforced the idea that computer security is not outside the mainstream of daily computing and computer support. Over time, I also added computer security responsibilities to the computer support staff's position descriptions and performance plans. Tasks assigned to computer specialists and assistants included:

* installing anti-virus software;

* installing an access warning message;

* installing password and access control software;

* conducting inventories of hardware and software;

* completing risk assessment documentation with user assistance;

* reviewing LAN, minicomputer, and the office access control system (Physical Access Control Management (PACMAN) System) audit logs; and

* interviewing users to develop a scenario from which to build a contingency plan.

## Discover the Value of Collateral-Duty Security Personnel

In order to spread the security workload throughout an agency, especially a large agency, computer security officers can promote the use of collateral-duty security personnel. Collateral-duty security personnel are those individuals appointed to provide part-time assistance to the computer security office. Collateral-duty appointees can assist in developing security plans, completing risk analyses, conducting hardware and software inventories, coordinating computer security training for system users, reviewing system audit trails, and reviewing user requests for access to systems.

Use of collateral-duty personnel in agencies allows the computer security officer to more effectively implement and maintain a security program. Collateral-duty personnel can be appointed in the following manner:

* Local Area Network (LAN) Security Officers: Each division, branch, and other organizational element which has a LAN, or is planning for the installation of a LAN, could appoint a LAN Security Officer. A system administrator for a LAN could also serve as the LAN Security Officer. The LAN Security Officer can be responsible to implement procedures designed to control access to the LAN, periodically check the LAN server(s) for viruses, perform regular backups, assist with risk analyses and contingency planning, provide basic security training to new users and periodic updates to regular users, and troubleshoot computer security problems.

* Information System Security Officers (ISSOs): ISSOs are made responsible for ensuring computer security policy and procedures are properly implemented. The system administrator for a minicomputer, server, World Wide Web site, firewall, or an e-mail system can serve as the ISSO for that system. Personnel in a data center who are

responsible for receiving user requests for system access, establishing accounts, and maintaining user IDs and passwords could be appointed as ISSOs to handle access control functions. Other individuals in the data center could also be appointed as ISSOs for specific systems and data center operations, such as the tape library. The supervisor or manager of a function that uses a number of microcomputers could be appointed as the ISSO of systems for which they are responsible. Some government agencies use titles of Office Automation Coordinator, Office Automation Security Officer, or Microcomputer Area Security Officer to differentiate between collateral-duty security positions responsible for microcomputers and those responsible for larger systems.

* Terminal Area Security Officers (TASOs): Divisions and other organizational elements with **only** remote terminals could appoint TASOs. The TASO can be responsible to implement procedures designed to control access to the terminal area and to troubleshoot computer security problems. The TASO could also serve as the data owner's or application owner's representative and request user access from the appropriate ISSO.

The title of the collateral-duty person is less important than assigning appropriate tasks to the correct individual. These responsibilities are best assigned to the individual who manages, administers, or otherwise has responsibility for the system. The collateral-duty person may be, or report to, the data owner, functional manager, or data processing service provider. The collateral-duty appointee and his or her management chain have a vested interest in the integrity and security of the system and its data.

In addition to appointing collateral-duty personnel for systems, networks, and terminals, some agencies have found it beneficial to establish a single point of contact for all computer security program administration at each division or major organization level. Some agencies use the title of Security Coordinator. In addition, agencies may consider establishing collateral-duty titles of Assistant ISSO and Assistant LAN Security Officer for those larger offices and agency divisions which have microcomputers and LANs throughout the organization.

Appointing Security Coordinators will allow the agency's computer security officer to distribute requests for accomplishment of computer security tasks to the directors of that agency's major organizational elements. The managers could pass the requirement to their Security Coordinators. Each Security Coordinator could determine whether the request for assistance was related to LAN, microcomputer, or terminal security. The Security Coordinator could then pass the request (or pass their own request) to the appropriate ISSO or LAN Security Officer, via the appropriate division, branch, or other element manager. It is important to utilize the agency's existing chain of command. In a large division, for example, the ISSO for microcomputers could pass the requirement to Assistant ISSOs who are appointed in each branch. The Assistant ISSOs would then work with supervisors and system users to accomplish the task(s). Security Coordinators also offer a way to pass on timely information on new threats, reminders about good practices, and can act as reviewers of policies and procedures.

Some federal agencies have found this heirarchy makes implementation and maintenance of policy, procedures, and practices more manageable, negates the possible impact of distances between some agency offices, and provides easier individual identification and auditability for the computer security officer.  Utilization of this method can help spread the workload more evenly among system users and system administrators.  This method can increase the agency-wide awareness of information systems security responsibilities, while utilizing the existing management structure.

Collateral-duty Security Coordinators, ISSOs and Assistant ISSOs, and LAN Security Officers and Assistant LAN Security Officers should be trained by the computer security officer.  The computer security officer may also want to do some training by contracting with an outside trainer, or by sending people to courses offered outside the agency.  Collateral-duty personnel responsibilities should be documented in the agency's computer security policy document(s).

Collateral-duty personnel can report to the computer security officer on information systems security matters, but should use the existing "chain of command" to return or forward documentation to the computer security office.  Likewise, the computer security officer can send requests for information and accomplishment of tasks to the directors of the major organization elements (e.g., divisions, directorates, offices).  It is crucial to the success of the computer security program that managers and supervisors be aware of what is being asked of their collateral-duty personnel, as well as the information being passed back to the computer security officer.

Some agencies have incorporated these collateral-duty responsibilities into position descriptions and performance standards.  This helps formalize the collateral-duty appointments.  It also helps to motivate and provide a basis to award appointees.

When agencies implement a formal program of appointing people to serve as collateral-duty support for the computer security program office, the program can, at times, appear to be running itself.  As the program matures, periodic requests by the computer security officer to collateral-duty appointees for information, completion of forms/surveys, or for the training needs of system users, are met without the initial responses, questions, or quarrels.  The collateral-duty people, in time, come to respond like extensions of the computer security office.

## Conclusion

All of this is not to say that there is an easy-to-follow recipe for success in building a computer security program.  Every good program needs five key elements:

(1) a stable security program management element;

(2) the existence of an agreed upon, published mission and functions

statement;

(3) the existence of comprehensive, organization-wide information systems security policies;

(4) a stable resource base; and

(5) the involvement of the computer security element in the strategic information technology decision-making process.

The key to achieving these elements is a business-oriented approach to integrating computer security into the organization's business or mission, and a healthy dosage of salemanship to make that approach meaningful to those who can integrate computer security into the organization's decision-making process. Once that is accomplished, spreading the work to the organizational elements through the effective use of computer system and network support people and collateral-duty security personnel will allow the security program to grow and mature, in step with the organization's business.